

**ABSTRACT OF THE DISCLOSURE**

5

**METHOD AND SYSTEM FOR  
FACILITATING PUBLIC KEY CREDENTIALS ACQUISITION**

10 A methodology is presented for securely acquiring  
and managing PKI credentials using an enterprise's  
pre-existing information technology. A management  
application places user information from a directory into  
a pre-registration record, which is sent to the user as  
an e-mail attachment. When the user views the e-mail  
message through a browser-type application that has  
15 built-in key generation and digital certificate  
management, the user may be prompted for additional  
information, such as passwords. The browser-type  
application then generates a public/private key pair and  
stores the private key in a secure local keystore while  
20 also securely sending the public key, authentication  
data, and pre-registration record to a  
registration/certificate authority. A public key  
certificate and an attribute certificate are then issued  
for the user, copies of which are published into the  
25 directory and returned to the user for storing within the  
user's secure local keystore. The certificates may then  
be used in typical manners.

TOP SECRET